UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/871,525	05/31/2001	David Makower	190309-1200	1053

7590 05/26/2005

Steven M. Haas
Fay, Sharpe, Fagan, Minnich & McKee, LLP
1100 Superior Avenue,
Seventh Floor
Cleveland, OH 44114

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/871,525	MAKOWER ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8 and 10-48 are pending in this office action, claim 9 is canceled.

2. Applicant's arguments, filed April 4, 2005, with respect to claims 1-8 and 10-48 have been considered but are moot in view of the new ground(s) of rejection.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-8, 10-37, and 41-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood et al. (U.S. Patent No. 6,668,322) in view of Tan et al. (U.S. Patent Publication No. 2001/0045451 A1).

Regarding claim 1, Wood et al. teaches a method for transparent sign-on in a client-server environment, the method comprising the steps of:

- Receiving an encrypted communication on an originating server from a client, the client using a browser (col. 7, lines 22-25);
- Sending an encrypted communication **including the challenge string** to a central sign-on server from the originating server (col. 11, lines 35-40);

- Receiving an encrypted communication on the originating server from the central sign-on server, wherein the communication received on the originating server includes a response to the communication sent to the central sign-on server (col. 11, line 43 through col. 12, line 20) **and a first parameter based on the recognizing**;
- **Initiating** a client session on the originating server (col. 14, lines 54-59); and
- Sending another encrypted communication to the central sign-on server from the originating server (col. 14, line 60 through col. 15, line 4).

Wood et al. does not teach **the originating server belonging to at least one federation of trusted originating servers, each trusted originating server in the federation trusting the other originating servers in the federation**; creating a challenge **string** at the originating server; **recognizing the client by the central sign-on server**; **receiving client authenticating information from the client using the browser if the received first parameter indicates no session present for the client on any of the servers in the federation of trusted originating servers**; **using client authenticating information provided in the response to the communication sent to the central sign-on server if the received first parameter indicates a session is present for the client on any of the servers in the federation of trusted originating servers**.

Tan et al. teaches **the originating server belonging to at least one federation of trusted originating servers, each trusted originating server in the federation trusting the other originating servers in the federation** (paragraph 0004); creating a challenge **string** at the originating server (paragraph 0013); **recognizing the client by the central sign-on server** (paragraph 0023, the access server authenticates the client); **receiving client authenticating information from the client using the browser if the received first parameter indicates no session present for the client on any of the servers in the federation of trusted originating servers** (paragraph 0023); **using client authenticating information provided in the response to the communication sent to the central sign-on server if the received first parameter indicates a session is present for the client on any of the servers in the federation of trusted originating servers** (paragraph 0025).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server belonging to a federation of servers, creating a challenge string, recognizing the client, receiving authentication information from the client if no session information exists, and using sign-on information to log onto different servers, as taught by Tan et al., with the method of Wood et al. It would have been obvious for such modifications because the steps of Tan et al. provides for single sign-on access to a federation of servers that allows an already authenticated user to gain access to another server without having to re-authenticate the user (see paragraph 0004 of Tan et al.).

Regarding claim 2, the combination of Wood et al. in view of Tan et al. teaches wherein the step of creating a challenge further comprises the step of recording on the originating server a URL requested by the client browser, a time at which the challenge was generated, and a federation identification (see col. 7, lines 9-18 of Wood et al. and paragraph 0025 of Tan et al.).

Regarding claim 3, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending an encrypted communication to a central sign-on server further comprises the steps of redirecting the client browser to the central sign-on server and sending to the central sign-on server the federation identification, the challenge, and a server identification (see col. 12, lines 21-24 of Wood et al.).

Regarding claim 4, the combination of Wood et al. in view of Tan et al. teaches wherein the step of receiving an encrypted communication on the originating server from the central sign-on server further comprises the step of receiving a digital signature of the central sign-on server for all information communicated from the central sign-on server (see col. 14, lines 54-59 of Wood et al.).

Regarding claim 5, the combination of Wood et al. in view of Tan et al. teaches wherein the step of receiving an encrypted communication on the originating server from the central sign-on server further comprises the step of receiving a redirection of the client browser on the originating server (see col. 12, lines 27-37 of Wood et al.).

Regarding claim 6, the combination of Wood et al. in view of Tan et al. teaches wherein the step of receiving a redirection of the client browser further comprises the steps of receiving the challenge, and the digital signature on all of the information communicated from the central sign-on server (see col. 10, lines 30-47 of Wood et al.).

Regarding claim 7, the combination of Wood et al. in view of Tan et al. teaches wherein **the recognizing step comprises recognizing the client by the central sign-on server based on a cookie having a unique value previously stored on the client browser by the central sign-on server** (see paragraph 0035 of Tan et al.).

Regarding claim 8, the combination of Wood et al. in view of Tan et al. teaches **further including the step of redirecting the client browser to a requested URL based on a successful transparent sign-on** (see paragraph 0026 of Tan et al.).

Regarding claim 10, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending another encrypted communication to the central sign-on server from the originating server further comprises the step of creating a digital signature on all information sent to the central sign-on server (see col. 14, lines 60-64 of Wood et al.).

Regarding claim 11, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending another encrypted communication to the central sign-on

server further comprises the step of sending the challenge, a session time-out value, a **second** parameter specifying that a session has been **initiated** on the originating server, a log-in identification of the client for which the session has been created, and the digital signature (see col. 14, lines 60-64 and fig. 4, ref. num 420 of Wood et al.).

Regarding claim 12, Wood et al. teaches a method for transparent sign-on in a client-server environment, the method comprising the steps of:

- Receiving an encrypted communication on a central sign-on server, wherein the communication is from **the** web server (col. 11, lines 35-40);
- Recognizing a client on the central sign-on server (col. 11, lines 25-34);
- Sending an encrypted communication to the web server from the central sign-on server (col. 11, line 43 through col. 12, line 20) **including a first parameter based on the recognizing**; and
- Receiving another encrypted communication **including web-server-created session information** on the central sign-on server from the web server (col. 14, line 60 through col. 15, line 4).

Wood et al. does not teach receiving an encrypted message **including a web-server-created challenge string;** recognizing **based on a previously initiated session on at least one of a federation of trusted servers, the web server comprising one of the trusted servers, each trusted server trusting the remaining trusted servers in the federation**.

Tan et al. teaches receiving an encrypted message **including a web-server-created challenge string** (paragraph 0013); recognizing **based on a previously initiated session on at least one of a federation of trusted servers** (paragraph 0023 and paragraph 0035), **the web server comprising one of the trusted servers, each trusted server trusting the remaining trusted servers in the federation** (paragraph 0004).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server belonging to a federation of servers, creating a challenge string, and recognizing the client, as taught by Tan et al., with the method of Wood et al. It would have been obvious for such modifications because the steps of Tan et al. provides for single sign-on access to a federation of servers that allows an already authenticated user to gain access to another server without having to re-authenticate the user (see paragraph 0004 of Tan et al.).

Regarding claim 13, the combination of Wood et al. in view of Tan et al. teaches wherein the step of receiving an encrypted communication on the central sign-on server from the web server comprises the steps of receiving a redirection of the client browser on the central sign-on server and receiving a federation identification, **the** challenge, an identification of the web server, and a digital signature of the web server (see col. 12, line 21-24 of Wood et al.).

Regarding claim 14, the combination of Wood et al. in view of Tan et al. teaches wherein the step of recognizing the client on the central sign-on server further comprises the steps of creating a cookie on the client browser and creating a record of the client on the central sign-on server (see col. 11, lines 25-34 of Wood et al.).

Regarding claim 15, the combination of Wood et al. in view of Tan et al. teaches wherein the step of creating a record of the client on the central sign-on server further comprises the step of using the cookie and the identification of the originating server as a concatenated primary key (see col. 11, lines 35-41 of Wood et al. and paragraph 0025 of Tan et al.).

Regarding claim 16, the combination of Wood et al. in view of Tan et al. teaches wherein the step of recognizing the client on the central sign-on server comprises the steps of accessing a cookie on the client browser and looking up the client on the central sign-in server based on the cookie (see col. 11, lines 25-34 of Wood et al.).

Regarding claim 17, the combination of Wood et al. in view of Tan et al. teaches wherein the step of looking up the client based on the cookie comprises looking up the challenge associated with the client session from a record on the central sign-on server (see col. 14, lines 6-13 of Wood et al. and paragraph 0025 of Tan et al.).

Regarding claim 18, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending an encrypted communication to the web server from the central sign-on server comprises the step of creating a digital signature for all information communicated to the web server (see col. 14, lines 54-59 of Wood et al.).

Regarding claim 19, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending an encrypted communication to the web server from the central sign-on server further comprises the steps of redirecting the client browser back to the web server and communicating the client log-in identification for the current client session, the challenge, and the digital signature (see col. 12, lines 27-37 of Wood et al.).

Regarding claim 20, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending an encrypted communication to the web server from the central sign-on server further comprises the steps of redirecting the client browser back to the web server and communicating **the first** parameter indicating that no session was present on the central sign-on server, the challenge, and the digital signature (see col. 10, lines 30-47 of Wood et al.).

Regarding claim 21, the combination of Wood et al. in view of Tan et al. teaches wherein the step of receiving another encrypted communication on the central sign-on server further comprises the steps of receiving an identification of the web server, **the**

challenge, a session time-out value, and a digital signature for all information sent to the central sign-on server (see col. 14, lines 60-64 of Wood et al.).

Regarding claim 22, the combination of Wood et al. in view of Tan et al. teaches wherein the step of receiving another encrypted communication on the central sign-on server further comprises receiving a **second** parameter specifying that a session has been created on the web server and a log-in identification of the client for which the session has been created (see col. 14, lines 60-64 and fig. 4, ref. num 420 of Wood et al.).

Regarding claim 23, the combination of Wood et al. in view of Tan et al. teaches further comprising the step of updating a record of the client session on the central sign-on server (see col. 14, lines 54-59 of Wood et al.).

Regarding claim 24, the combination of Wood et al. in view of Tan et al. teaches wherein the step of updating a record of the client session on the central sign-on server comprises the step of verifying a digital signature of the web server (see col. 13, lines 60-67 of Wood et al.).

Regarding claim 25, the combination of Wood et al. in view of Tan et al. teaches wherein the step of updating a record of the client session on a central sign-on server

further comprises the steps of creating a record on the central sign-on server of the client session and the session time-out value (see col. 14, lines 34-54 of Wood et al.).

Regarding claim 26, Wood et al. teaches a method for session maintenance in a transparent sign-on client-server environment, the method comprising the steps of:

- Running a session freshening task for sessions on **each** web server (col. 15, line 47 through col. 16, line 15);
- Sending an encrypted communication to a central sign-on server from **each** web server (col. 11, lines 35-40); and
- Recognizing **an associated** session on the central sign-on server (col. 11, lines 25-34).

Wood et al. does not teach **a plurality of web servers, each web server comprising a trusted server included in a federation of trusted servers, each trusted server trusting the remaining trusted servers in the federation**; and sending an encrypted message **including a web-server-created challenge string**.

Tan et al. teaches **a plurality of web servers, each web server comprising a trusted server included in a federation of trusted servers, each trusted server trusting the remaining trusted servers in the federation** (paragraph 0004); sending an encrypted message **including a web-server-created challenge string** (paragraph 0013).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server belonging to a federation of servers, sending an encrypted message including a server created challenge string, as taught by Tan et al., with the method of Wood et al. It would have been obvious for such modifications because the steps of Tan et al. provides for single sign-on access to a federation of servers that allows an already authenticated user to gain access to another server without having to re-authenticate the user (see paragraph 0004 of Tan et al.).

Regarding claim 27, the combination of Wood et al. in view of Tan et al. teaches wherein the step of running a session freshening task comprises the steps of looking up a list of active sessions on the web server and determining whether a session will expire on the central sign-on server before the next time the session freshening task runs (see col. 16, lines 2-15 of Wood et al.).

Regarding claim 28, the combination of Wood et al. in view of Tan et al. teaches wherein the step of sending an encrypted communication to the central sign-on server from the web server comprises the step of sending a server identification of the web server, the challenge used in creating the session, a new time-out value for the session, and a digital signature for all information sent in the message (see col. 14, lines 60-64 of Wood et al.).

Regarding claim 29, the combination of Wood et al. in view of Tan et al. teaches wherein the step of recognizing a session on the central sign-on server comprises the steps of verifying the digital signature and using the challenge to look up a record of the sessions on the central sign-on server (see col. 11, lines 25-34 of Wood et al.).

Regarding claim 30, the combination of Wood et al. in view of Tan et al. teaches further comprising the step of updating a client session record associated with the session on the central sign-on server (see col. 14, lines 54-59 of Wood et al.).

Regarding claim 31, the combination of Wood et al. in view of Tan et al. teaches wherein the step of updating a client session record comprises the step of updating a time-out value for the session on the central sign-on server (see col. 16, lines 2-15 of Wood et al.).

Regarding claim 32, Wood et al. teaches a method for session maintenance in a transparent sign-on client server environment, the method comprising the steps of:

- Recognizing a client on a web server (col. 7, lines 22-25);
- Terminating a client session on the web server (fig. 2, ref. num 212);
- Sending an encrypted message to a central sign-on server (col. 11, lines 35-40);
- Recognizing the client on the central sign-on server (col. 11, lines 25-34);
- Updating a record of a session associated with the client (col. 14, lines 54-59); and

- Terminating **the** local session associated with the client at the second **trusted** web server (fig. 2, ref. num 212).

Wood et al. does not teach **the web server belonging to at least one federation of trusted web servers, each trusted web server trusting the remaining web servers in the federation, sending an encrypted message including a web-server-created challenge string**; sending an encrypted communication **from the central sign-on server** to a second **trusted** web server, the second **trusted** web server having a current local session associated with the client.

Tan et al. teaches **the web server belonging to at least one federation of trusted web servers, each trusted web server trusting the remaining web servers in the federation** (paragraph 0004), **sending an encrypted message including a web-server-created challenge string** (paragraph 0013); sending an encrypted communication **from the central sign-on server** to a second **trusted** web server, the second **trusted** web server having a current local session associated with the client (paragraph 0025).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server belonging to a federation of servers, sending an encrypted message including a server challenge string, and using sign-on information to log onto different servers, as taught by Tan et al., with the method of

Wood et al. It would have been obvious for such modifications because the steps of Tan et al. provides for single sign-on access to a federation of servers that allows an already authenticated user to gain access to another server without having to re-authenticate the user (see paragraph 0004 of Tan et al.).

Regarding claim 33, the combination of Wood et al. in view of Tan et al. teaches wherein the step of recognizing the client on the web server comprises the step of looking up **the web-server-created** challenge associated with a client session (see col. 14, lines 6-16 of Wood et al.).

Regarding claim 34, the combination of Wood et al. in view of Tan et al. teaches wherein the step of recognizing the client on the web server comprises receiving a communication from the client (see col. 7, lines 22-25 of Wood et al.).

Regarding claim 35, the combination of Wood et al. in view of Tan et al. teaches wherein a digital signature is created for all information communicated to the central sign-on server (see col. 14, lines 60-64 of Wood et al.).

Regarding claim 36, the combination of Wood et al. in view of Tan et al. teaches wherein the step of recognizing the client on the central sign-on server comprises the steps of verifying the digital signature of the web server and using the challenge to look

up a record of any current session associated with the client (see col. 14, lines 6-13 of Wood et al.).

Regarding claim 37, the combination of Wood et al. in view of Tan et al. teaches wherein the step of updating a record of a session associated with the client comprises deleting a record on the central sign-on server (see col. 6, lines 23-43 of Wood et al.).

Regarding claim 41, Wood et al. teaches a system for secure single sign-on in a client-server environment, the system comprising:

- A central sign-on server, the central sign-on server configured to communicate with the **at least one** client and **each** server (fig. 1, ref. num 120 and 140); and
- Means for identifying the **at least one** client on the central sign-on server (col. 11, lines 25-34).

Wood et al. does not teach a **plurality of** servers, **each** server configured to communicate with **at least one** client, **each server being a member of at least one federation of trusted servers, each trusted server trusting the remaining servers in the federation**; and **to receive a server-created challenge string from the communicating server**.

Tan et al. teaches a **plurality of** servers, **each** server configured to communicate with **at least one** client (fig. 1, ref. num 14, 18, 20, 22), **each server being a member**

of at least one federation of trusted servers, each trusted server trusting the remaining servers in the federation (paragraph 0004); and **to receive a server-created challenge string from the communicating server** (paragraph 0013).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server belonging to a federation of servers, receiving a server created challenge string, as taught by Tan et al., with the method of Wood et al. It would have been obvious for such modifications because the steps of Tan et al. provides for single sign-on access to a federation of servers that allows an already authenticated user to gain access to another server without having to re-authenticate the user (see paragraph 0004 of Tan et al.).

Regarding claim 42, the combination of Wood et al. in view of Tan et al. teaches wherein the means for identifying the client on the central sign-on server comprises **application code and script residing at** a Single Sign-on Support URL located on **each** server (see col. 12, lines 27-37 of Wood et al.) **and known by the central sign-on server**.

Regarding claim 43, the combination of Wood et al. in view of Tan et al. teaches wherein the Single Sign-on Support URL comprises means for creating **the** challenge when the client initiates communication with the server, means for redirecting the client browser to the central sign-on server, means for communicating the challenge to the

central sign-on server, and means for receiving a communication from the central sign-on server (see col. 7, lines 1-18 and col. 12, lines 21-24 and col. 11, lines 35-40 and col. 11, line 43 through col. 12, line 20 of Wood et al.).

Regarding claim 44, the combination of Wood et al. in view of Tan et al. teaches wherein the server and the central sign-on server are co-located on the same server (see col. 21, lines 31-42 of Wood et al.).

Claim Rejections - 35 USC § 103

5. Claims 38-40 and 45-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood et al. (USPN '322) in view of Tan et al. (USPN '123), and further in view of McCanne (U.S. Patent No. 6,785,704).

Regarding claim 38, the combination of Wood et al. in view of Tan et al. teaches all the limitations of claim 32, above. However, the combination of Wood et al. in view of Tan et al. does not teach wherein the step of sending an encrypted message to a second **trusted** web server further comprises sending the encrypted message to each web server for which the central sign-on server has a record of an active session associated with the client.

McCanne teaches wherein the step of sending an encrypted message to a second **trusted** web server further comprises sending the encrypted message to each

web server for which the central sign-on server has a record of an active session associated with the client (fig. 6, ref. num 54).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine sending the message to each web server for which the central sign-on server has a record of, as taught by McCanne, with the method of Wood et al./Tan et al. It would have been obvious for such modifications because each server needs the updated session.

Regarding claim 39, the combination of Wood et al. in view of Tan et al./McCanne teaches wherein the step of sending an encrypted message to a second **trusted** web server further comprises the step of sending a parameter indicating that the client session is terminated and a digital signature of the central sign-on server (see col. 10, lines 30-47 of Wood et al.).

Regarding claim 40, the combination of Wood et al. in view of Tan et al./McCanne teaches wherein the step of terminating a local session associated with the client at the second **trusted** web further comprises the step of verifying the digital signature of the central sign-on server (see col. 13, lines 60-67 of Wood et al.).

Regarding claim 45, the combination of Wood et al. in view of Tan et al. teaches all the limitations of claim 41, above. However, the combination of Wood et al. in view

of Tan et al. does not teach wherein each member of the federation of **trusted** servers is configured with a server identification, and configured to use a similar policy with regard to session management as a second server in the federation of **trusted** servers.

McCanne teaches wherein each member of the federation of **trusted** servers is configured with a server identification, and configured to use a similar policy with regard to session management as a second server in the federation of **trusted** servers (fig. 6, ref. num 54 and col. 12, lines 28-47).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server is a member of a federation of servers, where each member has a server identification, as taught by McCanne, with the system of Wood et al./Tan et al. It would have been obvious for such modifications because the array of servers provides scalability; the server identification uniquely identifies the individual servers.

Regarding claim 46, the combination of Wood et al. in view of Tan et al./McCanne teaches wherein **each** server in the federation of **trusted** servers is configured to send encrypted messages to the central sign-on server and receive encrypted messages from the central sign-on server (see col. 11, lines 35-40 and col. 11, line 43 through col. 12, line 20 of Wood et al.).

Regarding claim 47, the combination of Wood et al. in view of Tan et al./McCanne teaches wherein the central sign-on server is a central sign-on server for more than one federation of **trusted** servers, each federation of **trusted** servers being configured with a unique federation identification (see fig. 2, ref. num 28 of McCanne).

Regarding claim 48, the combination of Wood et al. in view of Tan et al./McCanne teaches wherein the central sign-on server is configured to create a digital signature that is recognized by the server in the federation of **trusted** servers (see col. 14, lines 54-59 of Wood et al.).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100